(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **06104900 A**

(43) Date of publication of application: **15 . 04 . 94**

(51) Int. Cl **H04L 12/28**
H04L 12/40

(21) Application number: **04252581**

(22) Date of filing: **22 . 09 . 92**

(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**

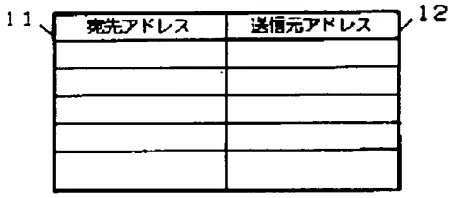
(72) Inventor: **KITO TSUTOMU**
YAMAGUCHI HIROSHI
NINOBE NAOHISA
TAKEUCHI HIRONORI
MORI TAKASHI
MUSA MUTSUMI

(54) LAN-TO-LAN CONNECTION METHOD

(57) Abstract:

PURPOSE: To provide LAN-to-LAN connection method capable of good filtering of high-class data realizing a security function which permits the access only to a specific terminal and inhibits the access to other terminals even when managing a LAN system.

CONSTITUTION: The method is provided with filtering table registerring a destination address 11 of the terminal equipment to which data are reached and a tramsission source address 12 of the terminal which sends the data. The connection is permitted to only inter-terminal equipment which is registered in the filtering table data connection request from an arbitrary terminal equipment, performing data transmission.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平6－104900

(43)公開日　平成６年(1994)４月15日

(51)Int.Cl.[5]	識別記号	庁内整理番号	Ｆ Ｉ		技術表示箇所
Ｈ０４Ｌ　12/28					
12/40					
		8732－5K	Ｈ０４Ｌ　11/ 00	３１０　Ｃ	
		7341－5K		３２０	

審査請求　未請求　請求項の数２(全　４　頁)

(21)出願番号　特願平4－252581

(22)出願日　平成４年(1992)９月22日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　鬼頭　勉
神奈川県横浜市港北区綱島東四丁目３番１号　松下通信工業株式会社内

(72)発明者　山口　広
神奈川県横浜市港北区綱島東四丁目３番１号　松下通信工業株式会社内

(72)発明者　ニ之部　直久
神奈川県横浜市港北区綱島東四丁目３番１号　松下通信工業株式会社内

(74)代理人　弁理士　小鍛治　明　（外２名）

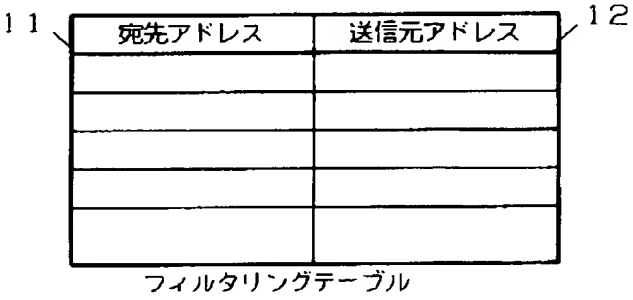
最終頁に続く

(54)【発明の名称】　ＬＡＮ間接続方法

(57)【要約】

【目的】　ＬＡＮシステムを管理する場合でも、特定の端末装置にのみアクセスし、他の端末装置にはアクセスを禁止できるセキュリティ機能を実現する、高度なデータのフィルタができる優れたＬＡＮ間接続方法を提供することを目的とする。

【構成】　データを到達すべき端末装置の宛先アドレス１１とデータを送出する端末装置の送信元アドレス１２とを登録するフィルタリングテーブルを設け、任意の端末装置からの接続要求に対して前記フィルタリングテーブルに登録された端末装置間にのみ接続を許可し、データの伝送を行う。



フィルタリングテーブル

1

【特許請求の範囲】

【請求項１】　それぞれ端末装置を接続する複数のＬＡＮ間で、データ伝送の経路を決定する宛先ＩＰアドレス及び送信元ＩＰアドレスを登録したルーティングテーブルを参照して接続し、任意のＬＡＮに接続された端末装置と他のＬＡＮに接続された端末装置との間でデータ伝送を行うときのＬＡＮ間接続方法であって、データを到達すべき端末装置の宛先アドレスとデータを送出する端末装置の送信元アドレスとを登録するフィルタリングテーブルを設け、任意の端末装置からの接続要求に対して前記フィルタリングテーブルに登録された端末装置間にのみ接続を許可し、データの伝送を行うことを特徴とするＬＡＮ間接続方法。

【請求項２】　それぞれ端末装置を接続する複数のＬＡＮ間で、データ伝送の経路を決定する宛先ＩＰアドレス及び送信元ＩＰアドレスを登録したルーティングテーブルを参照して接続し、任意のＬＡＮに接続された端末装置と他のＬＡＮに接続された端末装置との間でデータ伝送を行うときのＬＡＮ間接続方法であって、データの伝送を禁止する端末装置のＩＰアドレスを登録するフィルタリングテーブルを設け、任意の端末装置からの接続要求に対して前記フィルタリングテーブルを参照し、前記フィルタリングテーブルに登録された端末装置への接続を禁止することを特徴とするＬＡＮ間接続方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はコンピュータネットワークに利用するＬＡＮ間接続方法に関する。

【０００２】

【従来の技術】図２は複数のＬＡＮ間を接続してデータ伝送を行うシステムの構成を示すものである。図２において、３１はデータ伝送に光ファイバーを使用したＦＤＤＩ－ＬＡＮのバックボーンＬＡＮ（以下、単にバックボーンという）であり、３２，３３は複数の異なるＬＡＮをバックボーン３１に接続するＬＡＮ間接続装置である。このＬＡＮ間接続装置３２，３３は、物理層とデータリンク層が異なる複数のＬＡＮを、共通のネットワーク層（第３層）で相互接続する。３４はＦＤＤＩ－ＬＡＮに接続されている共通データベースである。３５，３６はＬＡＮを構成するイーサネットである。イーサネット３５及び３６には、端末装置３７Ａ，３７Ｂ及び３８Ａ，３８Ｂ、並びに、図には示してない他の端末装置が接続されている。

【０００３】図２のようなシステムにおいて、異なるＬＡＮに接続された端末装置間でデータの伝送を行う場合、自由にデータ伝送を行うわけではなく、ＩＰ（インターネットプロトコル）に基づいて、データの透過又は遮断を制御するフィルタリングを行うＬＡＮ間接続方法が用いられていた。

【０００４】従来のＬＡＮ間接続方法においてフィルタリングを行う場合に、ＩＰが本来保持しているルーティングテーブルをルーティングプロトコルを通して、もしくは、ルーティングプロトコルのコンフィグレーションを変更して、間接的にルーティングテーブルを書き換えるか、あるいは、ルーティングプロトコルを使用せずに直接、ルーティングテーブルを書き換えるというものであった。図３はルーティングテーブルを示すもので、１は宛先ＩＰアドレスであり、２は送信元ＩＰアドレスである。このＩＰアドレスは、Ａ，Ｂ，Ｃの３つのクラスを示すビットの他、上位のネットワークアドレス、及び、下位のホストアドレスで構成されている。

2

【０００５】次に上記従来例の動作について説明する。いま、端末装置３７Ａから端末装置３８ＢにＩＰデータを伝送する場合を想定する。まず、端末装置３７ＡからＩＰデータがＬＡＮ間接続装置３２に到達すると、ＬＡＮ間接続装置３２は、ＩＰデータを送信する宛先を、図３の宛先ＩＰアドレスを参照して検索する。そしてホストアドレスが同じイーサネット３５にあれば、そのＩＰデータを廃棄する。この場合、ホストアドレスの示す端末装置３８Ｂはイーサネット３５にないので、端末装置３８Ｂが接続されたＬＡＮ（イーサネットに限らない）をネットワークアドレスにより検索する。次に、をが存在するかどうかを、図３の宛先ＩＰアドレスの欄について検索する。この場合、データを伝送すべき端末装置２８Ｂが接続されたネットワークはイーサネット３６であるので、イーサネット３６に接続されているＬＡＮ間接続装置３３を宛先ＩＰアドレスとして、ＩＰデータを伝送する。これを受信したＬＡＮ間接続装置３３は、宛先ＩＰアドレスのホストアドレスが示す端末装置３８ＢにＩＰデータを伝送する。

【０００６】ＬＡＮ間接続装置３２又は３３において、ルーティングテーブルを参照した結果、一致するＩＰアドレスがエントリされていない場合には、そのデータは廃棄される。このように、上記従来のＬＡＮ間接続方法においてもＩＰデータのフィルタリングが実現されていた。

【０００７】

【発明が解決しようとする課題】しかしながら、上記従来のＬＡＮ間接続方法においては、ＩＰの本来もつルーティングテーブルに依存したフィルタ機能を用いているので、パスワード等のステーションレベルすなわちレイヤ２レベルでのセキュリティは可能であったが、レイヤ３レベルでのセキュリティとしては不十分であった。従って、１つのビル内に複数のテナントがそれぞれＬＡＮを構築している場合には、そのビル全体のＬＡＮシステムの管理者は、管理する全てのＬＡＮに接続された端末装置のアドレスを有するルーティングテーブルをもっている。従って、管理者は全ての端末装置に自由にアクセスすることができた。そのため、データの盗難やハッカーの侵入を防止することができず、完全なセキュリティ

を実現するには不十分であるという問題があった。

【０００８】本発明はこのような従来の問題を解決するものであり、ＬＡＮシステムを管理する場合でも、特定の端末装置にのみアクセスし、他の端末装置にはアクセスを禁止できるセキュリティ機能を実現する、高度なデータのフィルタができる優れたＬＡＮ間接続方法を提供することを目的とするものである。

【０００９】

【課題を解決するための手段】本発明は上記目的を達成するために、データを到達すべき端末装置の宛先アドレスとデータを送出する端末装置の送信元アドレスとを登録するフィルタリングテーブルを設け、任意の端末装置からの接続要求に対して前記フィルタリングテーブルに登録された端末装置間にのみ接続を許可し、データの伝送を行う。

【００１０】また、データの伝送を禁止する端末装置のＩＰアドレスを登録するフィルタリングテーブルを設け、任意の端末装置からの接続要求に対して前記フィルタリングテーブルを参照し、前記フィルタリングテーブルに登録された端末装置への接続を禁止する。

【００１１】

【作用】本発明は上記のような構成により、ＬＡＮ間接続装置を通過するデータがＩＰアドレスの組み合わせから、宛先もしくは送信元のネットワークアドレスでフィルタが掛けられるために高度なセキュリティ機能を実現するネットワーク設計が可能になる。

【００１２】

【実施例】以下、本発明の実施例を図２に示す構成を援用して説明する。

【００１３】本実施例において、共通データベース３４は、各イーサネット３５及び３６からアクセス可能にするが、他のイーサネットにアクセス可能な端末装置をイーサネットごとに制限するような構成とする。例えば、イーサネット３５では、端末装置３７Ａに限り他のイーサネットにアクセス可能とする。また、イーサネット３６では、端末装置３８Ａに限り他のイーサネットにアクセス可能とする。この場合には、ＬＡＮ間接続装置３２に設けたフィルタリングテーブルにおいて、宛先アドレスを３８Ａとし、送信元アドレスを３７Ａとする。同様に、ＬＡＮ間接続装置３３に設けたフィルタリングテーブルにおいて、宛先アドレスを３７Ａとし、送信元アドレスを３８Ａとする。

【００１４】このようなエントリを行うことにより、例えば、端末装置３８Ｂから端末装置３７Ａにアクセスしても接続を行わない。また、送信元アドレスが端末装置３８Ａ以外の端末装置場合にも、そのデータをフィルタリングすなわち遮断することができる。従って、このフィルタリングテーブルによってアクセス可能な端末装置を、例えば、トラヒックや課金情報等の管理データのみを格納する部門サーバとして、他の端末装置へはアクセスを禁止することができる。

【００１５】このように上記実施例によれば、従来のルーティングテーブルによっては行えないレイヤ３レベルでのフィルタリングが可能であり、データの盗難やハッカーの侵入を防止することができ、状況に応じたセキュリテイの要請に応えたネットワークの通信経路設計が可能になるという効果を得ることができる。

【００１６】なお、上記実施例においては、接続する端末装置のアドレスをエントリするようにしたが、接続を禁止する端末装置すなわちフィルタリングする端末装置のアドレスをエントリすることにより、エントリした端末装置以外のものに対して、データを伝送する構成としても良い。

【００１７】

【発明の効果】本発明は上記実施例より明らかなように、データを伝送する宛先アドレスと送信元アドレスをエントリするフィルタリングテーブルを設けることにより、レイヤ３レベルのセキュリティが可能となり、データの盗難やハッカーの侵入を防止でき、ウィルスの感染をも防御できる優れたＬＡＮ間接続方法を実現する効果が得られる。

【図面の簡単な説明】

【図１】本発明のＬＡＮ間接続方法に用いるフィルタリングテーブルの図

【図２】複数のＬＡＮ間を接続するシステムの構成図

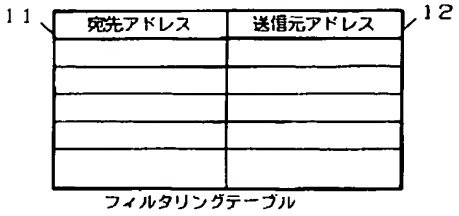
【図３】従来のＬＡＮ間接続方法に用いるルーティングテーブルの図

【符号の説明】

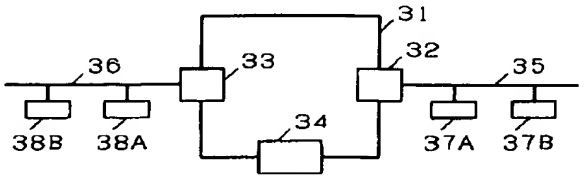
１１　宛先アドレス

１２　送信元アドレス

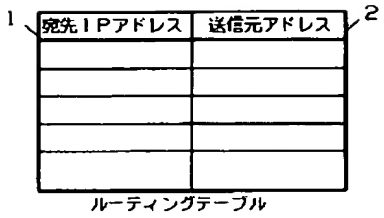
【図１】



【図２】



【図３】



ルーティングテーブル

フロントページの続き

(72)発明者　竹内　宏則
神奈川県横浜市港北区網島東四丁目３番１号　松下通信工業株式会社内

(72)発明者　森　孝志
神奈川県横浜市港北区網島東四丁目３番１号　松下通信工業株式会社内

(72)発明者　武佐　睦
神奈川県横浜市港北区網島東四丁目３番１号　松下通信工業株式会社内